基于 OpenVPN 的广播电视远程监测系统搭建与实现

张先辉
（国家广播电视总局 282 台，湖南 长沙 410146）

摘　要：随着计算机、网络等技术的快速发展，远程桌面控制作为一项重要的技术手段，在各领域中已经得到了广泛应用。为了保障广播电视的安全播出和正确的宣传导向，广播电视监测系统的搭建和技术完善必不可少。随着广播电视监测业务的要求越来越高，如何构建一个合适的广域网远程监测系统成为一个迫切需要解决的问题。本文结合 OpenVPN 的特点，提出了一个构建广域网远程监测系统环境的方案，完成系统的设计并实现。

关键词：OpenVPN；广域网；广播电视监测；远程桌面控制；系统搭建　　**中图分类号：**TN946　　**文献标识码：**A
文章编号：1671-0134（2022）06-151-03　　DOI：10.19483/j.cnki.11-4653/n.2022.06.045
本文著录格式：张先辉 . 基于 OpenVPN 的广播电视远程监测系统搭建与实现 [J]. 中国传媒科技，2022（06）：151-153.

导语

近年来广播电视传输的方式越来越多样化，广播电视监测范围也在不断扩大，很多监测业务需要通过互联网来实现，诸如 IPTV 用户终端、有线数字电视、互联网电视等。互联网环境不同导致播出的节目也有所不同，相关监管部门需要定期对不同的节目源进行实地收测、取证、抓包、分析等，耗费了不少的人力资源和时间成本。本文基于 OpenVPN 提出了一个远程监测方案，该方案适用于对 IPTV 用户终端、有线数字电视、互联网电视等进行远程监测，同时也解决了上述人力和时间成本的问题。本文对 OpenVPN 的特点进行简要分析，并搭建一个基于 Windows 系统的 OpenVPN 远程控制监测系统。

1.OpenVPN 简介

虚拟私有网络（VPN）就是一个专用的虚拟网络通道，通过该技术将两个不同地理位置的网络安全地连接起来，提供给企业之间或者个人与公司之间的一种安全的通讯线路，类似于内网专线。和传统的 VPN 相比，OpenVPN 的性能良好且稳定，系统搭建和使用简单友好，维护也相对方便，便于相关技术人员学习使用。OpenVPN 使用共享密钥、数字证书进行身份验证，这些都是根据用户自身需求利用软件自带的脚本工具配置的。利用 OpenSSL 加密库对通讯进行加密和证书管理，能够在 Windows、Linux 等常用系统上使用，它包含了许多诸如访问控制、加密、可用性管理等安全可靠的功能，已经不再是一个单纯的经过加密的网络通讯线路，而是一个可以解决广播电视远程监测系统网络环境的较优的方案。

1.1　虚拟网卡

虚拟网卡是 OpenVPN 的主要技术核心，依靠 tun/tap 驱动来实现其功能，除不具备物理网卡的硬件功能外，其他功能是一模一样的。其中包含了网卡处理驱动和字符设备驱动，负责在内核网络、物理网卡和用户之间传输数据。利用网卡驱动部分 tun 设备模拟网络行为处理网络数据，接收来自 TCP/IP 的数据或者将数据发送给 TCP/IP 进行处理。而字符设备驱动 tap 设备读写数据链路层完成与应用层的数据传送，将数据在内核网络和用户之间传送。OpenVPN 虚拟网卡工作过程如下。

1.1.1　发送数据过程

①应用程序发送网络数据；

②经过路由决策，网络数据传到内核网络协议栈做处理，再传输到虚拟网卡；

③数据通过虚拟网卡进入数据队列被 OpenVPN 读取并写入到网络协议栈；

④网络协议栈对数据进行封装等处理，然后转发给物理网卡；

⑤物理网卡处理并发送数据。

1.1.2　接收数据过程

①物理网卡接收到数据，对比特流进行解析，将得到的数据写入内核网络协议栈；

②应用层通过字符设备驱动，把数据传给驱动网卡；

③数据通过虚拟网卡 netif_rx（）接收程序重新进入协议栈；

④协议栈把数据传输至上层的应用程序。

虚拟网卡工作流程如图 2-1 所示。

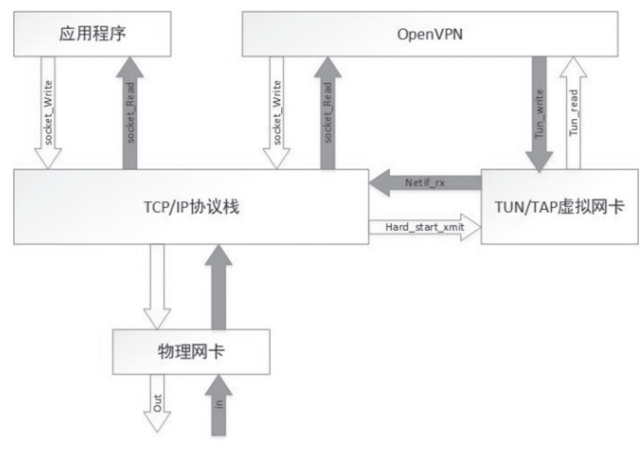


图 2-1　虚拟网卡工作流程

1.2　SSL/TLS 加密

SSL/TLS 最初叫作 SSL 协议，是“Secure Sockets Layer”英文的缩写，是一种安全套接字协议，共推出了 1.0、2.0、3.0 三个版本，广泛用于当今的互联网。随着 SSL 协议在互联网中的应用愈发广泛，已然成为互联网的安全标准。后来 IETF 组织将 SSL3.0 协议进行改进，便有了 TLS 协议（Transport Layer Security）的问世，但后来人们将其统称为 SSL/TLS 协议。该协议通过握手方式进行参数协商，诸如加密算法、认证算法、摘要算法、密钥配送算法等，通过握手制定出相同的加密算法和秘钥等相关加密信息，核心步骤很简单，双方确立加密算法并各自生成一个公钥和一个私钥，并交换公钥用于非对称加密算法，为接下来的通讯进行加密，也可以复杂一点添加 HASH 算法等。这样就在开放的互联网环境中实现加密通信，从而实现安全可靠的信息传递，让双方可以安心的说悄悄话。目前 SSL/TLS 应用最多的地方是与 HTTP（超文本传输协议）结合成 HTTPS（带加密技术的 HTTP），HTTP 很容易被窃听，而经过 SSL 协议加密的 HTTPS 通讯即使被窃听，通讯内容也不会被轻易破解解读。

2.OpenVPN 远程控制环境的构建

2.1 OpenVPN 服务器搭建与安装

这一部分是服务器设备跟客户端设备都要做的工作，操作基本相似。通过 OpenVPN 的官网或者其他安全途径下载最新的安装包 openvpn-install-2.4.6-I602.exe，安装在服务器和客户端的计算机中，安装过程中要注意需要勾选添加 easy-rsa，安装完成以后，会在 easy-rsa 目录下生成 OpenVPN 相关证书、秘钥制作的命令脚本等相关工具。

2.2 证书生成

搭建基于 OpenVPN 的远程监测系统，大部分和重要的工作都需要在服务器设备上进行，客户端方面较服务器端少了几个步骤，相对简单一些。服务器采用 RSA 非对称加密的算法和 CA 证书的验证方式对客户端进行验证，在默认的情况下一个客户端和服务器对应一个证书、秘钥等加密套件。所以第一步要做的就是证书和秘钥的制作。证书和秘钥的制作需要在服务器端进行，从证书制作工具（easy-rsa 文件夹）找到 vars.bat.sample 文件，用写字板打开，这里需要设置环境变量、证书及密钥生成命令的基础信息，如国家、机构等，可依据单位信息进行编辑，如表 2-1 所示。

表 2-1 证书密钥默认值

配置文件相关参数	注释
set KEY_COUNTRY=CN	// 国家
set KEY_PROVINCE=HN	// 省份
set KEY_CITY=CS	// 城市
set KEY_ORG=OpenVPN	// 组织
set KEY_EMAIL=mail@host.domain	// 邮件地址

编辑完成后使用 init-config 命令进行初始化。easy-rsa 目录下能看到安装自带的制作证书、秘钥等可能要用到的批处理文件，接下来依次制作 CA 证书文件、服务器证书和秘钥文件以及相应的客户端证书和秘钥文件，如表 2-2 所示。制作完成后，会在 easy-rsa\keys 目录下生成刚刚制作的相关证书和秘钥文件。

表 2-2 生成证书和密钥命令

制作证书、秘钥等相关 dos 命令	注释
init-config	// 初始化
clean-all	// 清空所有证书
build-ca	// 生成根证书和根私钥
build-key-server server01	// 为名为 server01 的服务器生成证书和服务器秘钥
build-key client01	// 为名为 client01 的客户端生成证书和客户端秘钥
build-dh	// 对生成的客户端证书进行 Diffie-Hellman 加密

2.3 建立配置文件

在安装目录 OpenVPN\sample-config 文件夹中找到 server.ovpn 文件并拷贝至服务器端 OpenVPN\config 文件夹中。将 client.ovpn 文件拷到客户端电脑安装目录下 OpenVPN\config 目录中，并根据自身对系统搭建的情况对文件关键部分进行编辑改写如表 2-3、表 2-4 所示。

表 2-3 OpenVPN 服务器端配置文件

配置文件相关参数	注释
port 1194	//OpenVPN 默认的端口号为 1194
proto udp	// 使用 UDP 协议
dev tun	// 使用 TUN 驱动
ca ca.crt	// 设置根 CA 证书，文件名根据实际文件名修改
cert server01.crt	// 设置服务器证书，文件名根据实际文件名修改
key server01.key	// 设置服务器密钥，文件名根据实际文件名修改
server 10.8.0.0 255.255.255.0	// 此处为服务器默认的虚拟 IP 地址与子网掩码，可根据自身情况进行编写更改
client-to-client	// 允许客户端和客户端之间相互访问
ifconfig-pool-persist ipp.txt	// 这是一个静态分配客户端地址的文件
push “redirect-gateway def1 bypass-dhcp”	// 客户端所有的网络连接都会通过服务器来实现

表 2–4 OpenVPN 客户端配置文件

配置文件相关参数	注释
proto udp	// 使用 UDP 协议
dev tun	// 使用 TUN 驱动
remote 47.100.xx.xx 1194	// 根据服务器设备的公网 IP 地址和端口号相关情况进行编写更改，默认端口号为 1194
ca ca.crt	// 设置根 CA 证书，文件名根据实际文件名修改
cert client01.crt	// 设置客户端证书，文件名根据实际文件名修改
key client01.key	// 设置服务器密钥，文件名根据实际文件名修改

2.4 配置文件分配

分配服务器证书（此操作在服务器设备上进行），将 keys 目录下 ca.crt、ca.key、dh2048.pem、server01.crt、server01.key、ta.key 这些文件存放到 OpenVPN\config 目录中，如图 2–1、图 2–2 所示。

01.pem	2019/1/9 22:41	PEM 文件	9 KB
02.pem	2019/1/9 22:50	PEM 文件	8 KB
ca.crt	2019/1/9 22:33	安全证书	3 KB
ca.key	2019/1/9 22:29	注册表项	4 KB
client01.crt	2019/1/9 22:50	安全证书	8 KB
client01.csr	2019/1/9 22:50	CSR 文件	2 KB
client01.key	2019/1/9 22:47	注册表项	4 KB
dh2048.pem	2019/1/9 22:45	PEM 文件	1 KB
index.txt	2019/1/9 22:50	文本文档	1 KB
index.txt.attr	2019/1/9 22:50	ATTR 文件	1 KB
serial	2019/1/9 22:50	文件	1 KB
server01.crt	2019/1/9 22:41	安全证书	9 KB
server01.csr	2019/1/9 22:41	CSR 文件	2 KB
server01.key	2019/1/9 22:37	注册表项	4 KB
ta.key	2019/1/10 0:36	注册表项	1 KB

图 2–1 keys 目录下的文件

此电脑 › 本地磁盘 (C:) › Program Files › OpenVPN › config

名称	修改日期	类型	大小
ca.crt	2019/1/9 22:33	安全证书	3 KB
ca.key	2019/1/9 22:29	注册表项	4 KB
dh2048.pem	2019/1/9 22:45	PEM 文件	1 KB
README.txt	2019/1/9 21:50	文本文档	1 KB
server.ovpn	2018/4/27 0:17	OpenVPN Confi...	11 KB
server01.crt	2019/1/9 22:41	安全证书	9 KB
server01.key	2019/1/9 22:37	注册表项	4 KB
ta.key	2019/1/10 0:36	注册表项	1 KB

图 2–2 将上述文件拷贝至服务器端该目录处

分配客户端证书的操作与分配服务器证书的操作相似，将服务器端 keys 目录下 ca.crt、client01.crt、client01.key、ta.key 文件拷贝到客户端安装目录 OpenVPN\config 下即可。

3. 系统测试情况

系统搭建安装完毕后，对某一地市的工控机进行连接测试，主要的测试内容是远程控制的速度与稳定性等。打开 OpenVPN GUI，测试服务器及客户端是否搭建安装完成。如图 3–1、图 3–2 所示。



图 3–1 OpenVPN 启动图标

OpenVPN Connection (server)

Current State: Connected

```
Thu Jan 10 01:00:40 2019 Route addition via service succeeded
Thu Jan 10 01:00:40 2019 Could not determine IPv4/IPv6 protocol. Using AF_INET6
Thu Jan 10 01:00:40 2019 Socket Buffers: R=[65536->65536] S=[65536->65536]
Thu Jan 10 01:00:40 2019 setsockopt(IPV6_V6ONLY=0)
Thu Jan 10 01:00:40 2019 UDPv6 link local (bound): [AF_INET6][undef]:1194
Thu Jan 10 01:00:40 2019 UDPv6 link remote: [AF_UNSPEC]
Thu Jan 10 01:00:40 2019 MULTI: multi_init called, r=256 v=256
Thu Jan 10 01:00:40 2019 IFCONFIG POOL: base=10.8.0.4 size=62, ipv6=0
Thu Jan 10 01:00:40 2019 IFCONFIG POOL LIST
Thu Jan 10 01:00:40 2019 Initialization Sequence Completed
Thu Jan 10 01:00:40 2019 MANAGEMENT: >STATE:1547053240,CONNECTED,SUCCESS,10.8.0.1,...
```

Assigned IP: 10.8.0.1

OpenVPN GUI 11.10.0.0/2.4.6

Disconnect | Reconnect | Hide

图 3–2 Open VPN 程序主页

见图 3–2，若搭建安装完成，则在 OpenVPN 程序主页，会看到分配的 ip，图标亮绿灯。

通过服务器端 OpenVPN 下 config 文件中的日志文件，可以查到通过 VPN 连接到此服务器的客户端 IP 等信息，如图 3–3 所示。

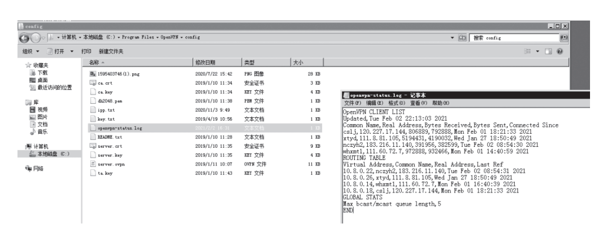


图 3–3 服务器端日志文件

根据文档中的 IP 地址信息远程连接客户端 10.8.0.14，见图 3–4。

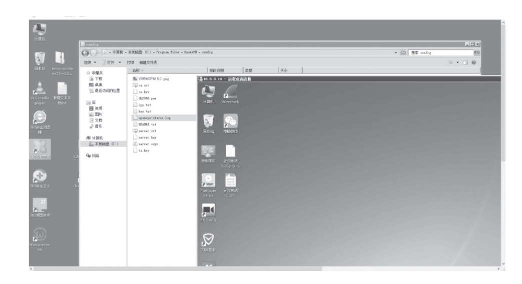


图 3–4 远程控制客户端界面

从连接测试环节可以看到，Open VPN 系统比较稳定，远程操作、画面回传都比较正常，能够顺利对前端 IPTV 用户终端设备、互联网电视机顶盒进行抓包，获取抓包信息文件传回本地进行分析，也能够对前端路由器、交换机、编码器等设备进行配置调试，保障了前端设备稳定运行，保证了业务顺利开展。

4. 总结

本文通过对 OpenVPN 的安装，在服务器和客户端上进行不同的操作配置，论述了 OpenVPN 远程控制环境的搭建过程。服务器与客户端的构建过程包含了安装 OpenVPN、建立 PKI（Public Key Infrastructure，公钥基础设施）、修改与分配配置文件四个步骤。此系统为监测系统的研发提供了新的思路和可行性，不仅可以实现远程 IPTV 用户终端、互联网电视、有线数字电视等监听监看相关任务，还可以随时对前端广播电视监测设备进行调试检修，极大地节省人员外出巡检带来的人力、财力、时间的成本。此外，该系统对环境的需求及技术门槛不高，操作起来非常方便，提高了前端广播电视监听监看的效率和稳定性。不过目前由于服务器设备性能及网络带宽的限制，还无法做到像内网专线那样流畅，后续会对服务器设备及网络方面进行升级优化，提高该系统的稳定性。媒

作者简介：张先辉（1992–），男，陕西西安，国家广播电视总局 282 台助理工程师，研究方向：互联网内容监管。

（责任编辑：李净）